# Reference Manual for the Broadband Voice Adapter TA612V

NETGEAR

**NETGEAR**, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10037-01
March 2005

© 2005 by NETGEAR, Inc. All rights reserved. March 2005.

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

EN 55 022 Declaration of Conformance

This is to certify that the TA612V Broadband Voice Adapter is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das TA612V Broadband Voice Adapter gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the TA612V Broadband Voice Adapter has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your TA612V Broadband Voice Adapter.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

## Product and Publication Details

| | |
|---|---|
| **Model Number:** | TA612V |
| **Publication Date:** | March 2005 |
| **Product Family:** | router |
| **Product Name:** | TA612V Broadband Voice Adapter |
| **Home or Business Product:** | Home |
| **Language:** | English |
| **Publication Part Number:** | 202-10037-01 |

# Contents

**Chapter 1**
**About This Manual**

Audience, Scope, Conventions, and Formats ..... 1-1
How to Use This Manual ..... 1-2
How to Print this Manual ..... 1-3

**Chapter 2**
**Introduction**

Key Features ..... 2-1
Voice Features ..... 2-2
A Powerful, True Firewall with Content Filtering ..... 2-2
Security ..... 2-2
Autosensing Ethernet Connections with Auto Uplink ..... 2-3
Extensive Protocol Support ..... 2-3
Easy Installation and Management ..... 2-4
Package Contents ..... 2-4
The Router's Front Panel ..... 2-5
The Router's Rear Panel ..... 2-6

**Chapter 3**
**Connecting the Router to the Internet**

Prepare to Install Your TA612V Broadband Voice Adapter ..... 3-1
First, Connect the TA612V Broadband Voice Adapter to Your Network ..... 3-1
Use the Smart Wizard to Configure Your TA612V Broadband Voice Adapter ..... 3-6
Setting up Your Voice Account ..... 3-9
Technical Support for Your Voice Account ..... 3-9
Troubleshooting Tips ..... 3-10
How to Manually Configure Your Internet Connection ..... 3-11

**Chapter 4**
**Content Filtering**

Blocking Access to Internet Sites ..... 4-1

Blocking Access to Internet Services ..... 4-2
Configuring E-Mail Alert and Web Access Log Notifications ..... 4-4
Viewing Logs of Web Access or Attempted Web Access ..... 4-6

**Chapter 5**
**Maintenance**

Viewing Status Information ..... 5-1
Viewing VoIP Status ..... 5-5
Viewing a List of Attached Devices ..... 5-7
Restoring Factory Defaults ..... 5-7
Changing the Administrator Password ..... 5-7
Backup Router Settings ..... 5-8

**Chapter 6**
**Advanced Configuration**

Configuring Port Triggering ..... 6-1
Configuring Port Forwarding to Local Servers ..... 6-3
Adding a Port Forwarding Custom Service ..... 6-5
Editing or Deleting a Port Forwarding Entry ..... 6-5
Local Web and FTP Server Example ..... 6-5
Multiple Computers for Half Life, KALI or Quake III Example ..... 6-6
Configuring WAN Setup Options ..... 6-6
Using LAN IP Setup Options ..... 6-9
Using the Router as a DHCP server ..... 6-10
Using Address Reservation ..... 6-11
How to Configure Static Routes ..... 6-12
Enabling Remote Management Access ..... 6-14
UPnP ..... 6-15
Syslog ..... 6-16
Firmware Upgrade ..... 6-17

**Chapter 7**
**Troubleshooting**

Basic Functioning ..... 7-1
Power Light Not On ..... 7-1
Lights Never Turn Off ..... 7-2
LAN or WAN Port Lights Not On ..... 7-2
Troubleshooting the Web Configuration Interface ..... 7-3

Troubleshooting the ISP Connection ..... 7-4
Troubleshooting a TCP/IP Network Using a Ping Utility ..... 7-5
Testing the LAN Path to Your Router ..... 7-5
Testing the Path from Your Computer to a Remote Device ..... 7-6
Restoring the Default Configuration and Password ..... 7-7
Problems with Date and Time ..... 7-7

**Appendix A**
**Technical Specifications**

**Appendix B**
**Network and Routing Basics**

Related Publications ..... B-1
Basic Router Concepts ..... B-1
What is a Router? ..... B-1
Routing Information Protocol ..... B-2
IP Addresses and the Internet ..... B-2
Netmask ..... B-4
Subnet Addressing ..... B-4
Private IP Addresses ..... B-7
Single IP Address Operation Using NAT ..... B-7
MAC Addresses and Address Resolution Protocol ..... B-8
Related Documents ..... B-9
Domain Name Server ..... B-9
IP Configuration by DHCP ..... B-10
Internet Security and Firewalls ..... B-10
What is a Firewall? ..... B-10
Stateful Packet Inspection ..... B-11
Denial of Service Attack ..... B-11
Ethernet Cabling ..... B-11
Category 5 Cable Quality ..... B-12
Inside Twisted Pair Cables ..... B-13
Uplink Switches, Crossover Cables, and MDI/MDIX Switching ..... B-14

**Appendix C**
**Preparing Your Network**

What You Need To Use a Router with a Broadband Modem ..... C-1
Cabling and Computer Hardware ..... C-1

Computer Network Configuration Requirements ..... C-1
Internet Configuration Requirements ..... C-2
Where Do I Get the Internet Configuration Parameters? ..... C-2
Record Your Internet Connection Information ..... C-3
Preparing Your Computers for TCP/IP Networking ..... C-3
Configuring Windows 95, 98, and Me for TCP/IP Networking ..... C-4
Install or Verify Windows Networking Components ..... C-4
Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me C-6
Selecting Windows' Internet Access Method ..... C-8
Verifying TCP/IP Properties ..... C-8
Configuring Windows NT4, 2000 or XP for IP Networking ..... C-9
Install or Verify Windows Networking Components ..... C-9
DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4 ..... C-10
DHCP Configuration of TCP/IP in Windows XP ..... C-10
DHCP Configuration of TCP/IP in Windows 2000 ..... C-12
DHCP Configuration of TCP/IP in Windows NT4 ..... C-15
Verifying TCP/IP Properties for Windows XP, 2000, and NT4 ..... C-17
Configuring the Macintosh for TCP/IP Networking ..... C-18
MacOS 8.6 or 9.x ..... C-18
MacOS X ..... C-18
Verifying TCP/IP Properties for Macintosh Computers ..... C-19
Verifying the Readiness of Your Internet Account ..... C-20
Are Login Protocols Used? ..... C-20
What Is Your Configuration Information? ..... C-20
Obtaining ISP Configuration Information for Windows Computers ..... C-21
Obtaining ISP Configuration Information for Macintosh Computers ..... C-22
Restarting the Network ..... C-23

**Glossary**

List of Glossary Terms ..... G-1

# Chapter 1
# About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

## Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.

This guide uses the following typographical conventions:

**Table 1-1. Typographical Conventions**

| | |
|---|---|
| *italics* | Emphasis, books, CDs, URL names |
| **bold** | User input |
| `fixed` | Screen text, file and server names, extensions, commands, IP addresses |

This guide uses the following formats to highlight special messages:

**Note:** This format is used to highlight information of importance or special interest.

This manual is written for the TA612V adapter according to these specifications:

**Table 1-2. Manual Scope**

| | |
|---|---|
| Product Version | TA612V Broadband Voice Adapter |
| Manual Publication Date | March 2005 |

**Note:** Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/TA612V.asp*.

# How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A TOC button that displays the table of contents and an Index button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A Knowledge Base button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

## How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  – Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

    Note: Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

  – Click the print icon in the upper left of the window.

    **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  – Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  – Click the print icon in the upper left of the window.

    **Tip**: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

# Chapter 2
# Introduction

Congratulations on your purchase of the NETGEAR® TA612V Broadband Voice Adapter. This chapter describes the features of the NETGEAR TA612V Broadband Voice Adapter.

## Key Features

The TA612V Broadband Voice Adapter connects your up two phones to your broadband Internet service. It connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem, and provides access to your local network.

The TA612V adapter provides you with multiple web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 252 computers. In addition to the Network Address Translation (NAT) feature, the built-in firewall protects you from hackers.

With minimum setup, you can install and use the router within minutes.

The TA612V adapter provides the following features:

- Two RJ-11 telephone lines.
- One Ethernet port of the built in 10/100 Mbps switch enable local computers to easily share access to the Internet.
- Voice over data prioritization ensures high-quality telephone service.
- Front panel LEDs for easy monitoring of status and activity.
- Permits simultaneous usage of phone lines and high speed data services.
- Flash memory for firmware upgrade.
- Easy, web-based setup for installation and management.
- Content Filtering and Site Blocking Security.
- Extensive Protocol Support.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.

## Voice Features

The TA612V Broadband Voice Adapter lets you use the full range of features in your voice account.

- Get your voicemail messages by phone, Web, or E-mail.
- Turn call waiting on or off. Easily switch between calls when you are using call waiting.
- Use Caller ID with any phone device that has Caller ID enabled. You can also block your Caller ID when you make a call.

## A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the TA612V is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection.

  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents.

  The TA612V will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to E-mail the log to you at specified intervals. You can also configure the router to send immediate alert messages to your E-mail address or E-mail pager whenever a significant event occurs.
- The TA612V prevents objectionable content from reaching your computers. The router allows you to control access to Internet content by screening for keywords within web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

## Security

The TA612V adapter is equipped with several features designed to maintain security, as described in this section.

- **Computers Hidden by NAT**: NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.
- **Port Forwarding**: Although NAT prevents Internet locations from directly accessing the computers on the LAN, the router allows you to direct incoming traffic to specific computers based on the service port number of the incoming request, or to one designated "DMZ" host computer. You can specify forwarding of single ports or ranges of ports.
- **Port Triggering**: Port Triggering is an advanced feature that can be used to easily enable gaming and other internet applications. Port Forwarding is typically used to enable similar functionality, but it is static and has some limitations.

## Autosensing Ethernet Connections with Auto Uplink

With its internal 3-port 10/100 switch, the TA612V can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The router incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection such as to a computer or an 'uplink' connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

## Extensive Protocol Support

The TA612V adapter supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to Appendix B, "Network and Routing Basics."

- **IP Address Sharing by NAT**: The TA612V adapter allows several networked computers to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.

- **Automatic Configuration of Attached computers by DHCP**: The TA612V adapter dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached computers on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of computers on your local network.
- **DNS Proxy**: When DHCP is enabled and no DNS addresses are specified, the router provides its own address as a DNS server to the attached computers. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**: PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as Entersys or WinPOET on your computer.

## Easy Installation and Management

You can install, configure, and operate the TA612V Broadband Voice Adapter within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**: Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based web Management Interface.
- **Smart Wizard**: The TA612V adapter Smart Wizard automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Visual monitoring**: The TA612V adapter's front panel LEDs provide an easy way to monitor its status and activity.

# Package Contents

The product package should contain the following items:

- TA612V Broadband Voice Adapter.
- Stand for vertically mounting the TA612V Broadband Voice Adapter
- AC power adapter.
- Category 5 (CAT5) Ethernet cable.
- *NETGEAR CD*, including:
  - This guide.

  – Application Notes and other helpful information.

- Support Registration card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the router for repair.

## The Router's Front Panel

The front panel of the TA612V adapter contains these status indicators.

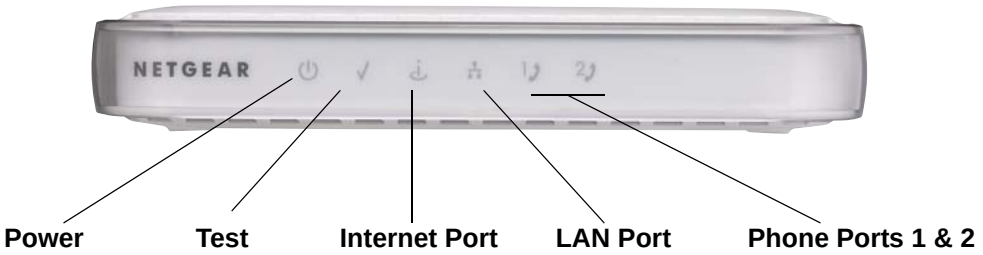



**Figure 2-1: TA612V Front Panel**

Viewed from left to right, the table below describes the lights on the front panel of the router.

**Table 2-1. Status Light Descriptions**

| Label | Activity | Description |
|---|---|---|
| Power | On Green Solid<br>Off | Power is supplied to the router.<br>Power is not supplied to the router. |
| Test | Blinking<br>Off | The router is performing its diagnostic test.<br>The router successfully completed its diagnostic test. |
| Internet Port | On<br>Blink | The Internet port has detected a link with an attached device.<br>Data is being transmitted or received by the Internet port. |
| LAN Port | Green<br>Amber<br>Blink | The LAN port has detected a 100 Mbps link with an attached device.<br>The LAN port has detected a 10 Mbps link with an attached device.<br>Data is being transmitted or received by the LAN port. |
| Phone Ports | Off<br>On<br>Blink | The phone port has not yet been provisioned by the service provider.<br>The phone port has been provisioned by the service provider.<br>There is a voice message waiting. |

## The Router's Rear Panel

The rear panel of the Model TA612V router contains the port connections listed below.

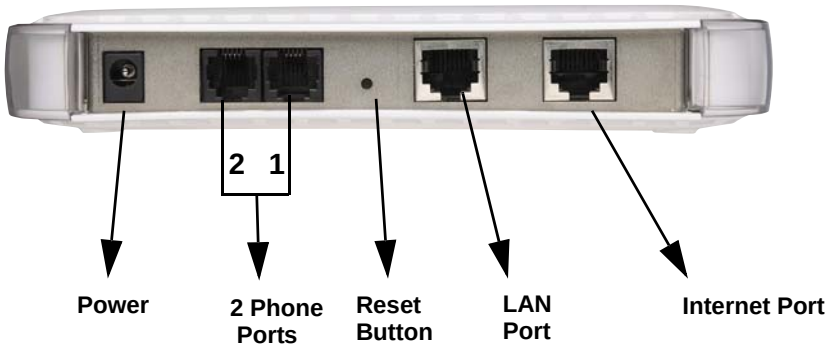



**Figure 1-2: TA612V Rear Panel**

Viewed from left to right, the rear panel contains the following features:

- Outlet for 12V DC @ 1.5A output AC power adapter
- Two phone ports
- Factory default reset push button for Restoring the Default Configuration and Password
- LAN port
- Internet (WAN) Ethernet port

# Chapter 3
# Connecting the Router to the Internet

This chapter describes how to set up the router on your local area network (LAN) and connect to the Internet. You will find out how to configure your broadband voice adapter for Internet access.

Follow these instructions to set up your router.

## Prepare to Install Your TA612V Broadband Voice Adapter

- *For Cable Modem Service*: When you perform the broadband voice adapter setup steps be sure to use the computer you first registered with your cable ISP.
- *For DSL Service*: You may need information such as the DSL login name/e-mail address and password in order to complete the broadband voice adapter setup.

Before proceeding with the broadband voice adapter installation, familiarize yourself with the contents of the Setup CD, especially this manual and the tutorials for configuring computers for networking.

## First, Connect the TA612V Broadband Voice Adapter to Your Network

### 1. CONNECT THE BROADBAND VOICE ADAPTER, THE COMPUTER, AND THE MODEM

a. Turn off your computer.

b. Turn off the cable or DSL broadband modem.

c. Locate the Ethernet cable (cable 1 in the diagram) that connects your PC to the modem.

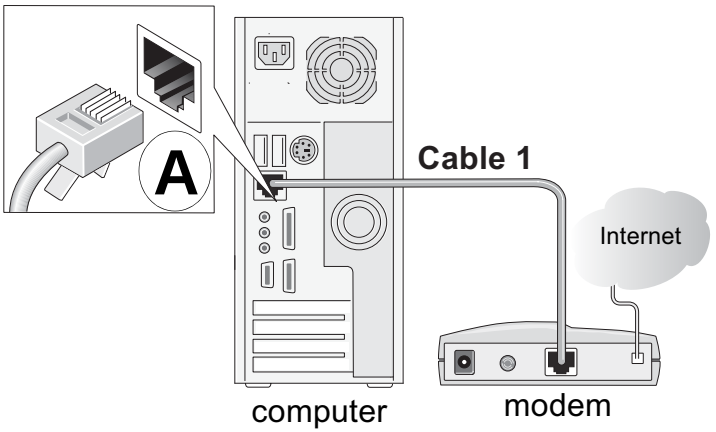



**Figure 3-1: Disconnect the Ethernet cable from the computer**

d. Disconnect the cable at the computer end only, point **A** in the diagram above.

e. Look at the label on the bottom of the broadband voice adapter. Locate the Internet port. Securely insert the Ethernet cable from your modem (cable 1 in the diagram below) into the Internet port of the broadband voice adapter as shown in point **B** of the diagram below.

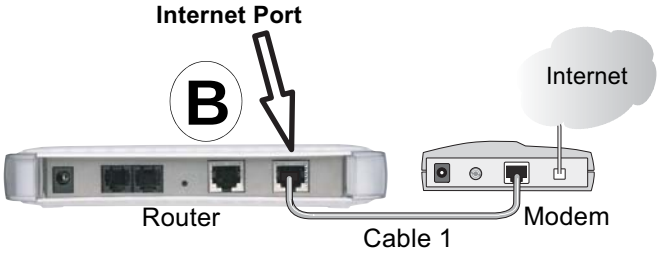



**Figure 3-2: Connect the broadband voice adapter to the modem**

**Note:** The stand provided with the broadband voice adapter provides a convenient, space-saving way of installing the broadband voice adapter. Avoid stacking it on other electronic equipment.

f. Securely insert the cable that came with your broadband voice adapter (the NETGEAR cable in the diagram below) into the LAN port on the router (point **C** in the diagram), and the other end into the Ethernet port of your computer (point **D** in the diagram).

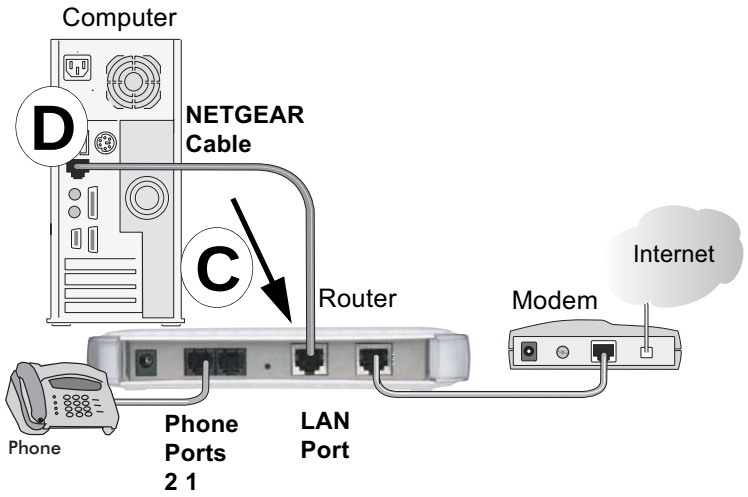



**Figure 3-3: Connect the computer to the broadband voice adapter**

If you have a voice service or plan to order it, connect a telephone to Phone Port 1 on the TA612V adapter using a standard phone cord (not included).

Your network cables are connected and you are ready to restart your network.

## 2. Restart your network in the correct sequence

**Warning:** Failure to restart your network in the correct sequence could prevent you from connecting to the Internet.

a. First, plug in and turn on the broadband modem. Wait about 2 minutes.

b. Now, plug in the power cord to your broadband voice adapter. Wait about 2 minutes.

c. Last, turn on your computer.

**Note**: For DSL customers, if software logs you in to the Internet, *do not* run that software. You may need to go to the Internet Explorer Tools menu, Internet Options, Connections tab page where you can select "Never dial a connection."

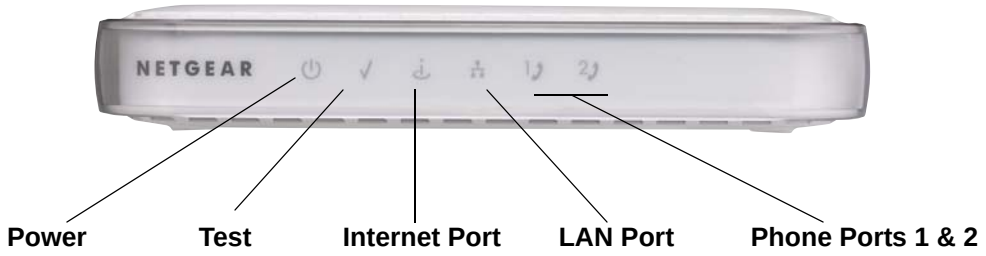



**Figure 3-4: Status lights on the broadband voice adapter**

d. Check the broadband voice adapter status lights to verify the following:

- *Power*: The power light should turn solid green. If it does not, see "Troubleshooting Tips" on page 3-10.
- *Test*: The test light should be off. The test light blinks when the router is first turned on then goes off. If after 2 minutes it is still on, see the Troubleshooting Tips below.
- *Internet*: The Internet port light should be lit. If not, make sure the Ethernet cable is securely attached to the broadband voice adapter Internet port and the modem, and the modem is powered on.
- *LAN*: A LAN light should be lit. Green indicates your computer is communicating at 100 Mbps; yellow indicates 10 Mbps. If a LAN light is not lit, check that the Ethernet cable from the computer to the router is securely attached at both ends, and that the computer is turned on.
- *Phone*: The Phone light will not be lit until your phone service provider provisions the phone service. Check the user guide from your phone service provider for details on provisioning the phone service.

## 3. Open a Browser and Log In to the Router

**For DSL customers**, if your Internet service provider had you install software logs you in to the Internet, *do not* run that software. If such software automatically starts when you open a browser, you may need to go to the Internet Explorer Tools menu, Internet Options, Connections tab page where you can select "Never dial a connection."

1. From the Ethernet connected computer you just set up, open a browser such as Internet Explorer or Netscape® Navigator.

2. Connect to the broadband voice adapter by typing **http://192.168.61.1** in the address field of your browser, then click **Enter**.

**Figure 3-5: Login address**

3. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password in lower case letters.

   **Note:** The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.

   A login window like the one shown below opens:

**Figure 3-6: Login window**

**Note**: If you cannot connect to the broadband voice adapter, verify your cables are connected correctly, that the router is powered on, and that the networking setup of your computer is set to obtain its settings automatically via DHCP. It should be set to obtain *both* IP and DNS server addresses automatically, which is usually so.

After logging in to the router, you will see the Internet connection Smart Wizard on the settings main page.

# Use the Smart Wizard to Configure Your TA612V Broadband Voice Adapter

Setup Wizard
Setup Wizard
The Smart Setup Wizard Can Detect The Type Of Internet Connection That You Have.
Do You Want The Smart Setup Wizard To Try And Detect The Connection Type Now?
Yes.
No, I Want To configure the router myself.
Next

**Figure 3-7: Setup wizard**

1. You are now connected to the router. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu.
2. Click **Next** to proceed. Input your ISP settings, as needed.

   **Note:** If you choose not to use the Setup Smart Wizard, you can manually configure your Internet connection settings by following the procedures in the Setup Manual on the CD.

   Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP.
3. When the router successfully detects an active Internet service, the router's Internet LED goes on. The Setup Smart Wizard reports which connection type it discovered, and displays the appropriate configuration menu. If the Setup Smart Wizard finds no connection, you will be prompted to check the physical connection between your router and the cable or DSL modem.
4. The Setup Smart Wizard will report the type of connection it finds and prompts you for the settings.
5. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection and register your product. If you have trouble connecting to the Internet, use the Basic Setup Troubleshooting Tips below to correct basic problems, or refer to the Setup Manual on the CD.

   You are now connected to the Internet! Next, configure your computer.

The Router Settings pages allow you to configure, upgrade and check the status of your NETGEAR Broadband Voice Router.

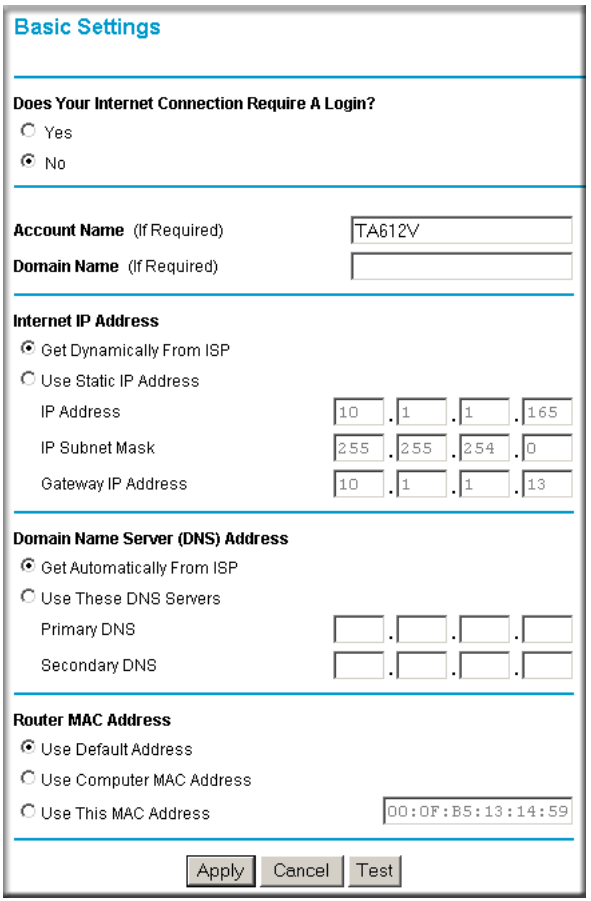



**Figure 3-8: Basic Settings page**

Helpful information related to the selected Settings page appears in this column. If you are using Internet Explorer, you may click an item in the center column to jump directly to the related help section; otherwise, scroll down until you reach it.

**Note**: If you are setting up the router for the first time, the default settings may work for you with no changes.

- Does Your Internet Connection Require A Login?

  Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select Yes. Otherwise, select No.

  **Note**: If you have installed PPP software such as WinPoET (from Earthlink) or Enternet (from PacBell), then you have PPPoE. Select Yes. After selecting Yes and configuring your router, you will not need to run the PPP software on your PC to connect to the Internet.

- Account Name (also known as Host Name or System Name): For most users, type your account name or user name in this box. For example, if your main mail account is JerAB@ISP.com, then put JerAB in this box. If your ISP has given you a specific Host name, then type it (for example, CCA7324-A).

- Domain Name: For most users, you may leave this box blank, unless required by your ISP. You may type the domain name of your ISP. For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the Domain Name.

  If you have a Domain name given to you by your ISP, type it in this box. (For example, Earthlink Cable may require a Host name of 'home' and Comcast sometimes supplies a Domain name.)

  If you have a cable modem, this is usually the Workgroup name.

- Internet IP Address: If you log in to your service or your ISP did not provide you with a fixed IP address, the router will find an IP address for you automatically when you connect. Select Get Dynamically From ISP.

  If you have a fixed (or static IP) address, your ISP will have provided you with the required information. Select Use Static IP Address and type the IP Address, Subnet Mask and Gateway IP Address into the correct boxes.

  For example:

  – IP Address: 24.218.156.183

  – Subnet Mask: 255.255.255.0

  – Gateway IP Address: 24.218.156.1

- DNS Address: The DNS server is used to look up site addresses based on their names.

  If your ISP gave you one or two DNS addresses, select Use These DNS Servers and type the primary and secondary addresses.

  Otherwise, select Get Automatically From ISP.

**Note**: If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers aren't set up properly. You should contact your ISP to get DNS server addresses.

- Router MAC Address: Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address.

  Usually, select Use Default MAC Address.

  If your ISP requires MAC authentication, then select either Use Computer MAC address to disguise the Router's MAC address with the Computer's own MAC address or Use This MAC Address to manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX. This value may be changed if the Use Computer MAC Address is selected once a value has already been set in the Use This MAC Address selection.

- Click Test to connect to the NETGEAR Web site. If you connect successfully, your settings work and you may click Logout to exit these pages and... enjoy surfing the 'net!
- If you don't connect successfully:

  a. Go through the settings and make sure you've selected the correct options and typed everything correctly.

  b. Contact your ISP to verify the configuration information.

  c. Read the Troubleshooting section in the Router Installation Guide.

  d. On the Resource CD, read the Troubleshooting Guide or the Troubleshooting section in the Reference Manual.

  e. Contact NETGEAR Technical Support.

## Setting up Your Voice Account

Refer to the Quick Installation Guide (QIG) provided by your Voice Service Provider.

## Technical Support for Your Voice Account

For technical support contact your Voice Service Provider.

# Troubleshooting Tips

Here are some tips for correcting simple problems you may have.

**Be sure to restart your network in this sequence:**

1. Turn off *and* unplug the modem, turn off the broadband voice adapter, and turn off the computer.
2. Turn on the modem, wait two minutes.
3. Turn on the broadband voice adapter and wait 1 minute.
4. Turn on the computer.

**Make sure the Ethernet cables are securely plugged in.**

- The Internet status light on the broadband voice adapter will be lit if the Ethernet cable to the broadband voice adapter from the modem is plugged in securely and the modem and broadband voice adapter are turned on.
- For each powered on computer connected to the broadband voice adapter with a securely plugged in Ethernet cable, the corresponding broadband voice adapter LAN port status light will be lit. The label on the bottom of the broadband voice adapter identifies the number of each LAN port.

**Make sure the network settings of the computer are correct.**

- LAN connected computers *must* be configured to obtain an IP address automatically via DHCP. Please see Appendix C, “Preparing Your Network or the animated tutorials on the CD for help with this.
- Some cable modem ISPs require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select “Use this Computer’s MAC Address.” The router will then capture and use the MAC address of the computer that you are now using. You must be using the computer that is registered with the ISP. Click **Apply** to save your settings. Restart the network in the correct sequence.

**Check the router status lights to verify correct router operation.**

- If the Power light does not turn solid green within 2 minutes after turning the router on, reset the router according to the instructions in “Restoring the Default Configuration and Password” on page 7-7.

# How to Manually Configure Your Internet Connection

You can manually configure your router using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

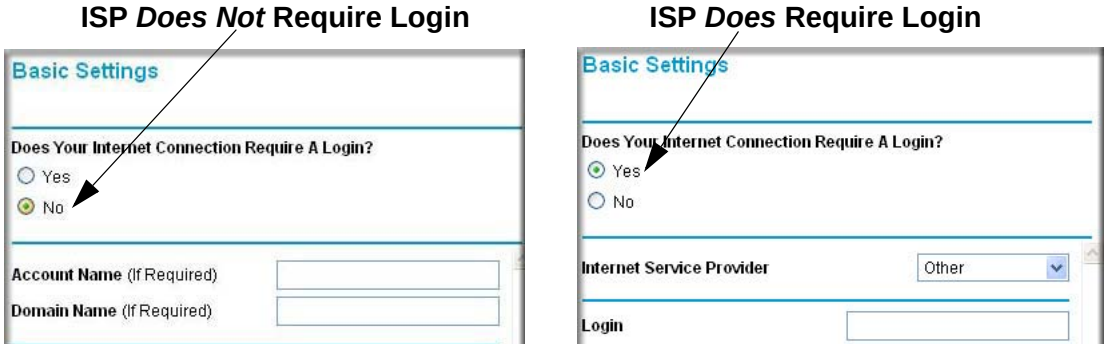



**Figure 3-9: Browser-based configuration Basic Settings menus**

You can manually configure the router using the Basic Settings menu shown in Figure 3-9 using these steps:

1. Connect to the broadband voice adapter by typing **http://192.168.61.1** in the address field of your browser, then click **Enter**.
2. For security reasons, the broadband voice adapter has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters.
3. Click **Basic Settings** on the Setup menu.
4. If your Internet connection does not require a login, click No at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click Yes, and skip to step 5.

    a. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.

    b. Internet IP Address:
    If your ISP has assigned you a permanent, fixed (static) IP address for your computer, select "Use static IP address". Enter the IP address that your ISP assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's router to which your router will connect.

c. Domain Name Server (DNS) Address:
If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

**Note:** If you enter an address here, restart the computers on your network so that these settings take effect.

d. Router's MAC Address:
This section determines the Ethernet MAC address that will be used by the router on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" its MAC address.

To change the MAC address, select "**Use this Computer's MAC address**." The router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Or, select "Use this MAC address" and type it in here.

e. Click **Apply** to save your settings.

5. If your Internet connection does require a login, fill in the settings according to the instructions below. Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

**Note:** After you finish setting up your router, you will no longer need to launch the ISP's login program on your computer in order to access the Internet. When you start an Internet application, your router will automatically log you in. Click **Apply** to save your settings. Click the Test button to verify you have Internet access.

# Chapter 4
# Content Filtering

This chapter describes how to use the content filtering features of the TA612V Broadband Voice Adapter to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

The TA612V Broadband Voice Adapter provides you with web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based web addresses and web address keywords. You can also block Internet access by applications and services, such as chat or games.

## Blocking Access to Internet Sites

The TA612V adapter allows you to restrict access based on web addresses and web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is below:

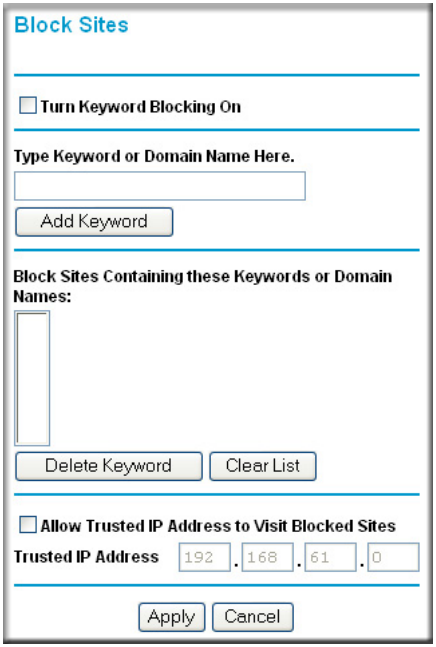



**Figure 4-1: Block Sites menu**

To enable keyword blocking, select either “Per Schedule” or “Always”, then click Apply. If you want to block by schedule, be sure that a time period is specified in the Schedule menu.

To add a keyword or domain, type it in the Keyword box, click Add Keyword, then click Apply.

To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access during a scheduled period, enter the keyword “.” and set the schedule in the Schedule menu.

To specify a Trusted User, enter that computer’s IP address in the Trusted User box and click Apply. You may specify one Trusted User, which is a computer that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that computer with a fixed IP address.

## Blocking Access to Internet Services

The TA612V adapter allows you to block the use of certain Internet services by computers on your network. This is called services blocking or port filtering. The Block Services menu is shown below:

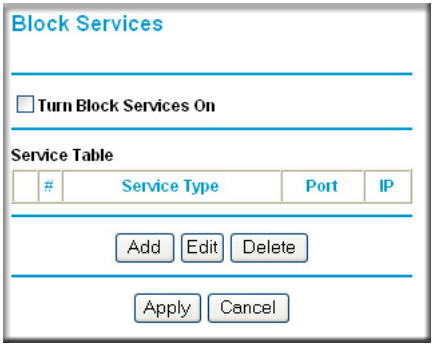



**Figure 4-2: Block Services menu**

Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

To specify a service for blocking, click Add. The Add Services menu will appear, as shown below:

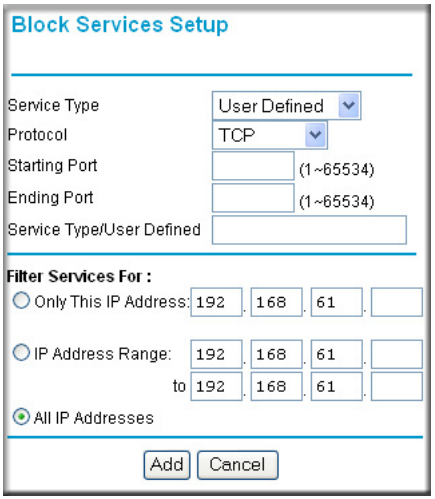



**Figure 4-3: Add Services menu**

From the Service Type list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select User Defined.

- **Configuring a User Defined Service**

To define a service, first you must determine which port number or range of numbers is used by the application. The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups.

Enter the Starting Port and Ending Port numbers. If the application uses a single port number, enter that number in both boxes.

If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select Both.

- **Configuring Services Blocking by IP Address Range**

Under “Filter Services For”, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

## Configuring E-Mail Alert and Web Access Log Notifications

In order to receive logs and alerts by email, you must provide your email information in the E-Mail menu, shown below:

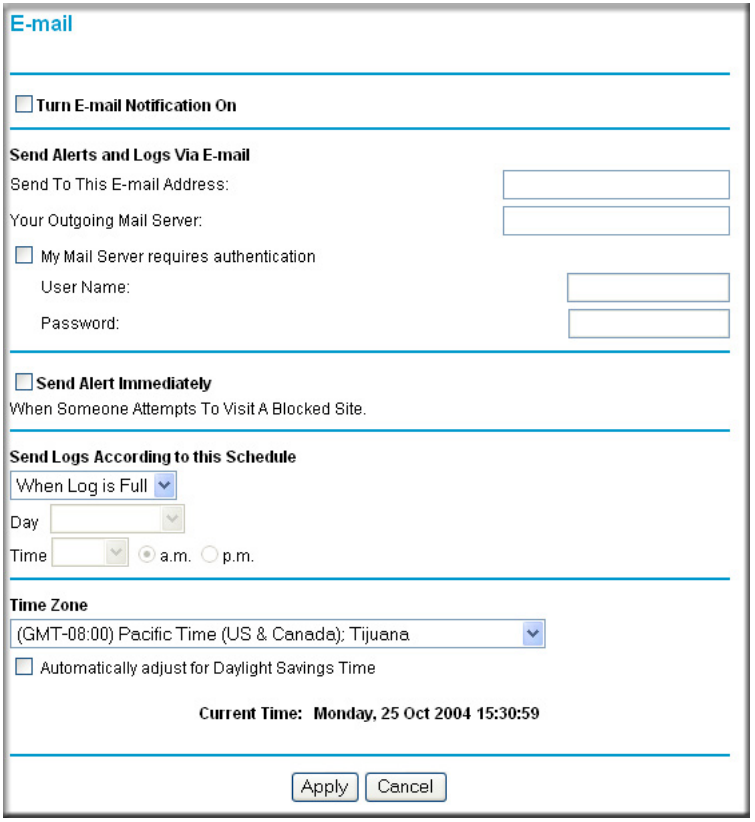



**Figure 4-4: Email menu**

- Turn e-mail notification on
  Check this box if you wish to receive e-mail logs and alerts from the router.
- Send to this e-mail address
  Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- Your outgoing mail server
  Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.
- My Mail Server Requires Authentication
  Select this checkbox and enter the user name and password for this email account, as required.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately
  Check this box if you would like immediate notification of attempted access to a blocked site.
- Send logs according to this schedule
  Specifies how often to send the logs: None, Hourly, Daily, Weekly, or When Full.
  - Day for sending log. Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents. If you don't want logs sent, select None from the list in the Send Logs According To This Schedule area. When you turn on e-mail notification and choose None in the Send Logs According to this Schedule list, the alert is sent but not the log.

The TA612V adapter uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Daylight Savings Time. Check this box to automatically adjust for daylight savings time.

# Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of what websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries will only appear when keyword blocking is enabled, and no log entries will be made for the Trusted User. An example is shown below:

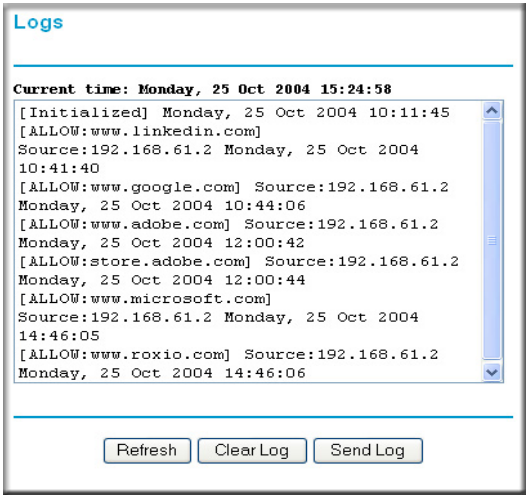



**Figure 4-5: Logs menu**

Log entries are described in Table 4-1

**Table 4-1. Log entry descriptions**

| Field | Description |
|---|---|
| Action | This field displays whether the access was blocked or allowed. |
| | The name or IP address of the website or newsgroup visited or attempted to access. |
| Date and Time | The date and time the log entry was recorded. |
| Source IP | The IP address of the initiating device for this log entry. |
| Date and Time | The date and time the log entry was recorded. |
| | |

Log action buttons are described in Table 4-2

**Table 4-2. Log action buttons**

| Field | Description |
|---|---|
| Refresh | Click this button to refresh the log screen. |
| Clear Log | Click this button to clear the log entries. |
| Send Log | Click this button to email the log immediately. |

# Chapter 5
# Maintenance

This chapter describes how to use the maintenance features of your TA612V Broadband Voice Adapter. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

## Viewing Status Information

The Router Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, click on Maintenance, then select System Status to view the System Status screen, shown below.

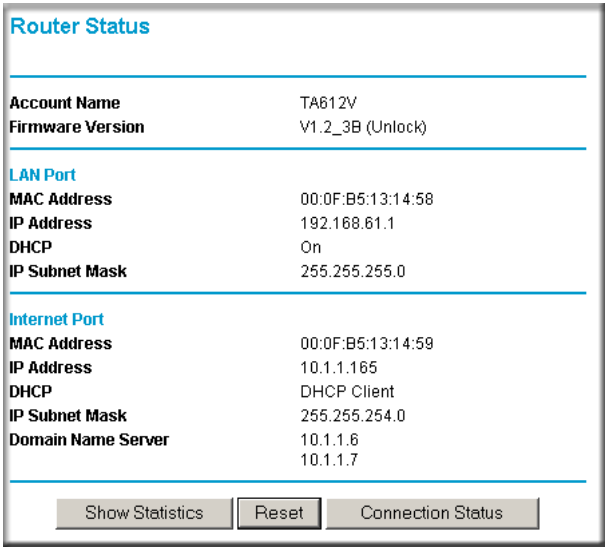



**Figure 5-1: Router Status screen**

This screen shows the following parameters:

**Table 5-1. Menu 3.2 - TA612V Broadband Voice Adapter Status Fields**

| Field | Description |
|---|---|
| Account Name | This field displays the Host Name assigned to the router. |
| Firmware Version | This field displays the router firmware version. |
| Internet Port | These parameters apply to the Internet (WAN) port of the router. |
| MAC Address | This field displays the Media Access Control address being used by the Internet (WAN) port of the router. |
| IP Address | This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet. |
| IP Subnet Mask | This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router. |
| DHCP | If set to None, the router is configured to use a fixed IP address on the WAN.<br>If set to Client, the router is configured to obtain an IP address dynamically from the ISP. |
| LAN Port | These parameters apply to the Local (WAN) port of the router. |
| MAC Address | This field displays the Media Access Control address being used by the LAN port of the router. |
| IP Address | This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.61.1 |
| DHCP | Identifies if the router's built-in DHCP server is active for the LAN attached devices. |
| IP Subnet Mask | This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0 |

Click on the “Connection Status” button to display the WAN status, as shown below.

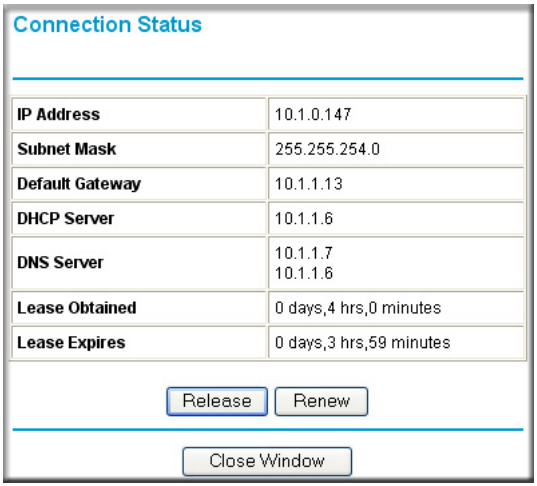



**Figure 5-2: Connection Status screen**

This screen shows the following statistics:.

**Table 5-1. Connection Status Fields**

| Field | Description |
|---|---|
| IP Address | The WAN (Internet) IP Address assigned to the router. |
| Subnet Mask | The WAN (Internet) Subnet Mask assigned to the router. |
| Default Gateway | The WAN (Internet) default gateway the router communicates with. |
| DHCP Server | The WAN (Internet) DHCP server address assigned to the router. |
| DNS Server | The WAN (Internet) DNS server addresses assigned to the router. |
| Default Gateway | The WAN (Internet) default gateway the router communicates with. |
| Lease Obtained | The time when the router got its DHCP lease from your Internet service provider’s network. |
| Lease Expires | The time when the DHCP lease expires. |

WAN Status action buttons are described in Table 5-2

**Table 5-2. Connection Status action buttons**

| Field | Description |
|---|---|
| Release | Click Release to release the DHCP lease. |
| Renew | Click Renew to renew the DHCP lease. |

Click on the "Show Statistics" button to display router usage statistics, as shown below.

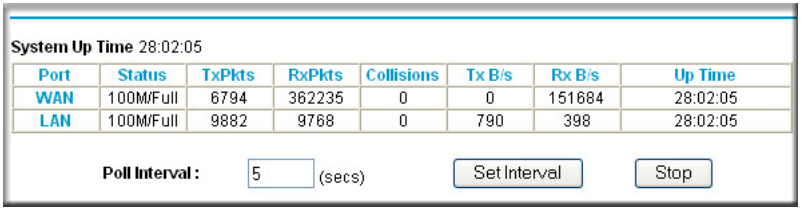

System Up Time 28:02:05
Port Status TxPkts RxPkts Collisions Tx B/s Rx B/s Up Time
WAN 100M/Full 6794 362235 0 0 151684 28:02:05
LAN 100M/Full 9882 9768 0 790 398 28:02:05
Poll Interval : 5 (secs)
Set Interval
Stop

**Figure 5-3: Router Statistics screen**

This screen shows the following statistics:

**Table 5-1. Router Statistics Fields**

| Field | Description |
|---|---|
| Port | The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays: |
| Status | The link status of the port. |
| TxPkts | The number of packets transmitted on this port since reset or manual clear. |
| RxPkts | The number of packets received on this port since reset or manual clear. |
| Collisions | The number of collisions on this port since reset or manual clear. |
| Tx B/s | The current transmission (outbound) bandwidth used on the WAN and LAN ports. |
| Rx B/s | The current reception (inbound) bandwidth used on the WAN and LAN ports. |
| Up Time | The amount of time since the router was last restarted. |
| Up Time | The time elapsed since this port acquired the link. |
| Poll Interval | Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display. |

Show Statistics action buttons are described in Table 5-2

**Table 5-2. Show Statistics action buttons**

| Field | Description |
|---|---|
| Set Interval | Enter a time and click the button to set the polling frequency. |
| Stop | Click the Stop button to freeze the polling information. |

# Viewing VoIP Status

This VoIP Status page shows the current status of your VoIP (Voice over Internet Protocol) connection.

**Figure 5-4: VoIP Status page**

- LAN Port
  - MAC Address - the physical address of the router, as seen from the local LAN.
- Line 1/Line 2
  - Display Name: This is the name you have already chosen when you first opened your account. Your "Display Name" will be visible to other individuals with caller ID.

    If your display name appears as "UNAVAILABLE", either your account has not been established or your router has been unable to connect to the Internet.
  - Telephone Number: This is the telephone number other people will use when they call you. This number was assigned to your router when you first established your account. Each line can have a different telephone number.

    If your Telephone Number appears as "phonenumber", either your account has not been established or your router has been unable to connect to the Internet.
- Line Status
  - Hook State: The "Hook State" displays the condition of the telephone receiver. ON indicates the receiver is "on-the-hook", while OFF indicates the receiver is "off-the-hook".
  - Registration State: When your router has successfully connected to the VoIP servers, the "Registration State" will be displayed as "Success". However, if you do not have a VOIP account or if the router could not connect to the VoIP servers, the "Registration State" will be displayed as "Idle".
  - Message Waiting: The "Message Waiting" status indicates if you have a new message waiting in your voice mail box.

# Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown below.

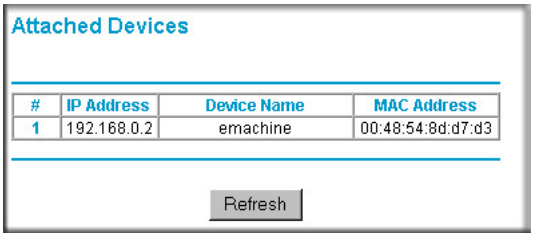



**Figure 5-5: Attached Devices menu**

For each device, the table shows the IP address, NetBIOS Host Name (if available), and Ethernet MAC address. Note that if the router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the Refresh button.

## Restoring Factory Defaults

The Restore Factory Defaults option in the Maintenance menu allows you to restore the router to the factory default settings. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be **password**, the LAN IP address will be 192.168.61.1, and the router's DHCP client will be enabled.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See “Restoring the Default Configuration and Password” on page 7-7.

# Changing the Administrator Password

The default password for the router’s web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password.

From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown below.

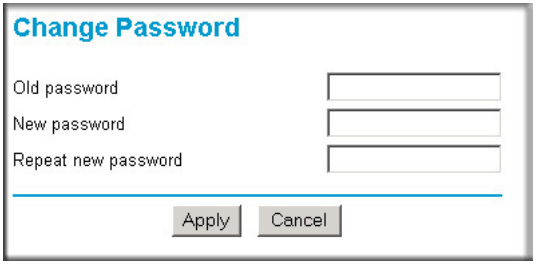



**Figure 5-6: Set Password menu**

To change the password, first enter the old password, and then enter the new password twice. Click Apply.

## Backup Router Settings

The Backup Settings page allows you to backup, restore and erase the router's current settings.

**Note**: Operations on this screen only affect the Router. The VoIP module is unaffected.

Once you have the router working properly, you should backup the information to have it available if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can restore the router's settings from this file.

**IMPORTANT**! Once you start restoring settings or erasing the router, do NOT try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! This should only take a minute or so. When the Test light stops blinking, wait a few more seconds before doing anything with the router.

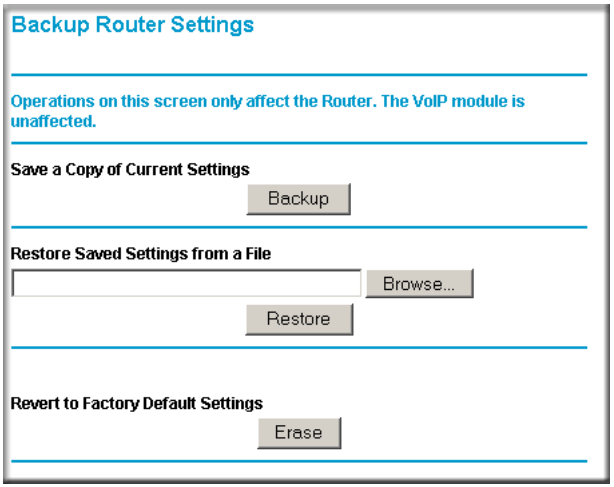

Backup Router Settings
Operations on this screen only affect the Router. The VoIP module is unaffected.
Save a Copy of Current Settings
Backup
Restore Saved Settings from a File
Browse...
Restore
Revert to Factory Default Settings
Erase

**Figure 5-7: Backup Router Settings page**

- Save (Backup): To create a backup file of the current settings:
  a. Click Backup.
  b. If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click Save.
  If you have your browser set up to save downloaded files automatically, the file is saved to the your browser's download location on the hard disk and is called netgear.cfg.
- Restore: To restore settings from a backup file:
  a. Click Browse.
  b. Locate and select the previously saved backup file (by default, netgear.cfg).
  c. Click Restore.

  A window appears letting you know that the router has been successfully restored to previous settings. The router will restart. This will take about one minute.

  **IMPORTANT**! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.
  d. Close the message window.

- Revert (Erase): To erase the current settings and reset the router to the original factory default settings:

  – Click Erase.

  **IMPORTANT**! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.

  After you have erased the router's current settings, the router's password will be password, the LAN IP address will be 192.168.61.1 and the router will act as a DHCP server on the LAN and act as a DHCP client to the Internet.

# Chapter 6
# Advanced Configuration

This chapter describes how to configure the advanced features of your TA612V Broadband Voice Adapter. These features can be found under the Advanced heading in the Main Menu of the browser interface.

## Configuring Port Triggering

Port Triggering is an advanced feature that can be used to easily enable gaming and other internet applications. Port Forwarding is typically used to enable similar functionality, but it is static and has some limitations.

Port Triggering opens an incoming port temporarily and does not require the server on the internet to track your IP address if it is changed by DHCP, for example.

Port Triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

Using the Port Triggering page, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CUseeMe).

Port Forwarding is designed for FTP, Web Server or other server based services. Once port forwarding is set up, request from Internet will be forwarded to the proper server. On the contrary, port triggering will only allow request from Internet after a designated port is 'triggered'. Port triggering applies to chat and Internet games.

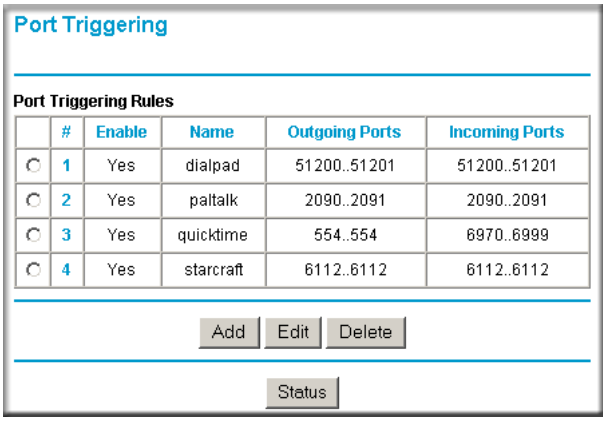

Port Triggering
Port Triggering Rules
# Enable Name Outgoing Ports Incoming Ports
1 Yes dialpad 51200..51201 51200..51201
2 Yes paltalk 2090..2091 2090..2091
3 Yes quicktime 554..554 6970..6999
4 Yes starcraft 6112..6112 6112..6112
Add Edit Delete
Status

**Figure 6-1: Port Triggering Menu**

**Note**: If Disable Port Triggering box is checked after configuring port triggering, port triggering will be disabled but any port triggering configuration information you added to the router will be retained even though it will not be used.

- Port Triggering Timeout

  Enter a value up to 9999 minutes. The Port Triggering Timeout value controls the inactivity timer for the designated inbound port(s). The inbound port(s) will be closed when the inactivity timer expires.

- For Internet Games or Applications

  Before starting, you'll need to know which service, application or game you'll be configuring. Also, you'll need to have the outbound port (triggering port) address for this game or application.

Follow these steps to set up a computer to play Internet games or use Internet applications:

1. Click **Add**.

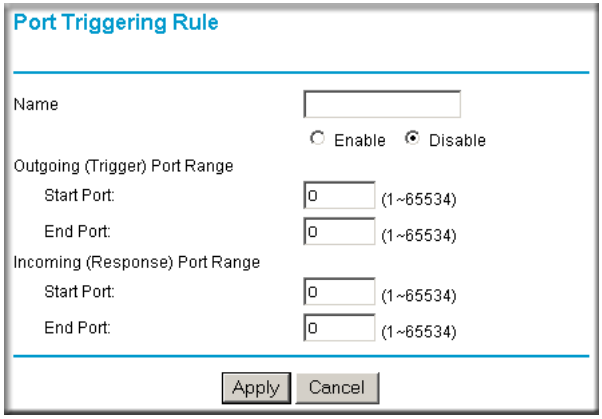



**Figure 6-2: Add Port Trigger Menu**

2. Enter a service name in the Service Name box.
3. Enter the outbound start and final port numbers.
4. Enter the inbound start and final port numbers. These port numbers can be obtained from the game or applications manual or support Web site.
5. Click **Apply** to save your changes.

## Configuring Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu. From the Main Menu of the browser

interface, under Advanced, click on Port Forwarding to view the port forwarding menu, shown below.

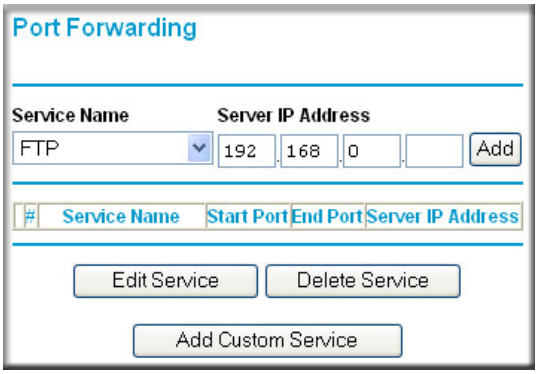



**Figure 6-3: Port Forwarding Menu**

**Note:** If you are unfamiliar with networking and routing, refer to Appendix B, "Network and Routing Basics," to become more familiar with the terms and procedures used in this manual.

Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the Security Menu.

Before starting, you'll need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. Be sure the computer's IP address never changes. To configure port forwarding to a local server:

**Note:** To assure that the same computer always has the same IP address, use the reserved IP address feature of your TA612V adapter. See "Using Address Reservation" on page 6-11 for instructions on how to use reserved IP addresses.

1. From the Service Name box, select the service or game that you will host on your network. If the service does not appear in the list, refer to the following section, "Adding a Port Forwarding Custom Service".
2. Enter the IP address of the local server in the corresponding Server IP Address box.

3. Click the Add button.

## Adding a Port Forwarding Custom Service

To define a service, game or application that does not appear in the Service Name list, you must determine what port numbers are used by the service. For this information, you may need to contact the manufacturer of the program that you wish to use. When you have the port number information, follow these steps:

1. Click **Add Custom Service**.
2. Enter the first port number in an unused Starting Port box.
3. To forward only one port, enter it again in the Ending Port box. To specify a range of ports, enter the last port to be forwarded in the End Port box.
4. Enter the IP address of the local server in the corresponding Server IP Address box.
5. Type a name for the service.
6. Click **Apply** to save your settings.

## Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry, follow these steps.

1. In the table, select the button next to the service name.
2. Click Edit or Delete.

## Local Web and FTP Server Example

If a local computer with a private IP address of 192.168.61.33 acts as a web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 192.168.61.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Maintenance Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account's IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.
- If the IP address of the local computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, you can manually configure the computer to use a fixed address.
- Local computers must access the local server using the computers' local LAN address (192.168.61.33 in this example). Attempts by local computers to access the server using the external IP address (172.16.1.23 in this example) will fail.

## Multiple Computers for Half Life, KALI or Quake III Example

To set up an additional computer to play Half Life, KALI or Quake III:

1. Click the button of an unused port in the table.
2. Select the game again from the Service Name list.
3. Change the beginning port number in the Start Port box.
   For these games, use the supplied number in the default listing and add +1 for each additional computer. For example, if you've already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.
5. Type the IP address of the additional computer in the Server IP Address box.
6. Click **Apply** to save your changes.

Some online games and videoconferencing applications are incompatible with NAT. The TA612V adapter is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default in the PORTS Menu. If one local computer acts as a game or videoconferencing host, enter its IP address as the default.

# Configuring WAN Setup Options

The WAN Setup options let you configure a DMZ server, change the MTU size and enable the broadband voice adapter to respond to a Ping on the WAN port. These options are discussed below.

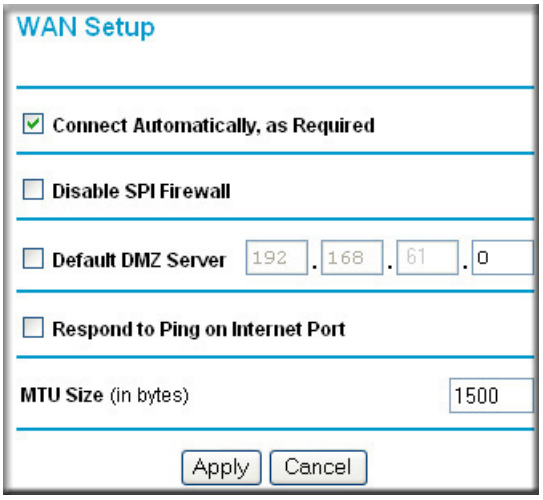



**Figure 6-4: WAN Setup menu.**

- **Connect Automatically, as Required**

  Normally, this option should be Enabled, so that an Internet connection will be made automatically, whenever Internet-bound traffic is detected. In locations where Internet access is billed by the minute, if this causes high connection costs, you can disable this setting.

  If disabled, you must connect manually, using the sub-screen accessed from the Router Status menu “Show WAN Status” screen.

- **Disable SPI Firewall**

  Normally, this option should be Enabled, so that your local network will be protected by the Stateful Packet Inspection (SPI) firewall included in the TA612V. However, certain communications functions like VPN may require turning off the SPI feature.

- **Setting Up a Default DMZ Server**

  The default DMZ server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer’s IP address is entered as the default DMZ server.

**Note:** DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The WAN Setup menu, shown below lets you configure a Default DMZ Server.

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Click **WAN Setup** on the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.
3. Click **Apply** to save your settings.

- **Respond to Ping on Internet WAN Port**

  If you want the router to respond to a 'ping' from the Internet, click the ‘Respond to Ping on Internet WAN Port’ check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Don't check this box unless you have a specific reason to do so.

- **Setting the MTU Size**

  The default MTU size is usually fine. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly some using PPPoE, you may need to reduce the MTU. This should not be done unless you are sure it is necessary for your ISP.

  Any packets sent through the router that are larger than the configured MTU size will be repackaged into smaller packets to meet the MTU requirement. To change the MTU size:

  Under MTU Size, enter a new size between 64 and 1500. Then, click Apply to save the new configuration.

# Using LAN IP Setup Options

The LAN IP Setup feature is under the Advanced heading of the main menu. This feature allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN IP Setup to view the LAN IP Setup menu, shown below.

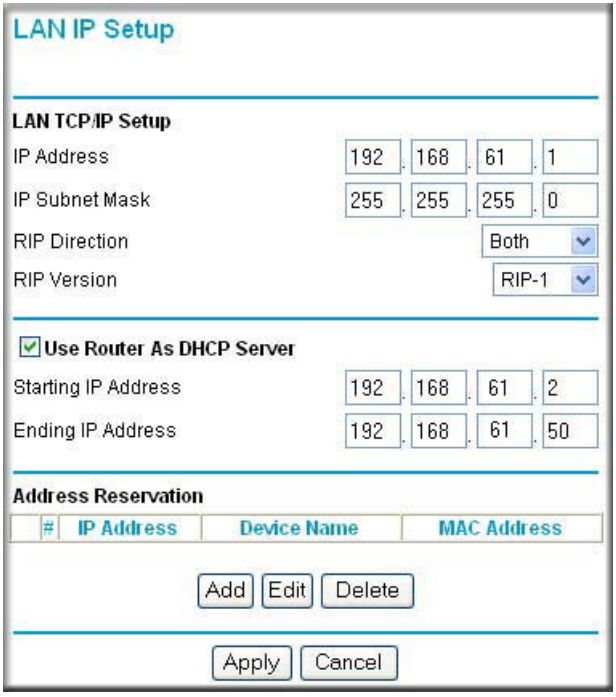



**Figure 6-5: LAN IP Setup Menu**

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The router's default LAN IP configuration is:

- LAN IP addresses—192.168.61.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- IP Address
  This is the LAN IP address of the router.
- IP Subnet Mask
  This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.
  - When set to Both or Out Only, the router will broadcast its routing table periodically.
  - When set to Both or In Only, it will incorporate the RIP information that it receives.
  - When set to None, it will not send any RIP packets and will ignore any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - RIP-2 carries more information. RIP-2B uses subnet broadcasting.

**Note:** If you change the LAN IP address of the router while connected through the browser, you will be disconnected. You may need to restart your computer for the new IP address setting to take effect.

## Using the Router as a DHCP server

By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached computers from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See "IP Configuration by DHCP" on page B-10 for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the 'Use router as DHCP server' check box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.61.1 and 192.168.61.253, although you may wish to save part of the range for devices with fixed addresses.

The router will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the router's LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router's LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu

## Using Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer will always receive the same IP address each time it access the router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click **Add**.
2. In the IP Address box, type the IP address to assign to the computer or server. (choose an IP address from the router's LAN subnet, such as 192.168.61.X)
3. Type the MAC Address of the computer or server. (Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click Edit or Delete.

## How to Configure Static Routes

Static Routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Route menu, shown below.

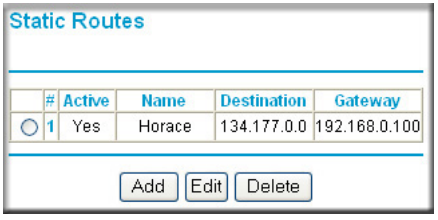



**Figure 6-6. Static Route Summary Table**

To add or edit a Static Route:

1. Click the Add button to open the Add/Edit Menu, shown below.

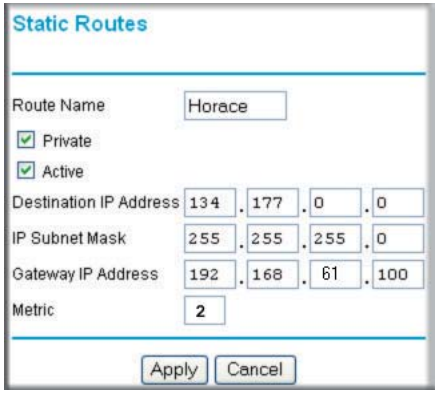



**Figure 6-7. Static Route Entry and Edit Menu**

2. Type a route name for this static route in the Route Name box under the table. (This is for identification purpose only.)
3. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select **Active** to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type 255.255.255.255.
7. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
8. Type a number between 1 and 15 as the Metric value.
   This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to have the static route entered into the table.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.61.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.61.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.61.100. The static route would look like Figure 6-7.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.0.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.61.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

## Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your TA612V adapter.

**Note:** Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for Remote Management:

1. Select the Turn Remote Management On check box.
2. Specify what external addresses will be allowed to access the router's remote management.

   **Note:** For enhanced security, restrict access to as few external IP addresses as practical.

   a. To allow access from any IP address on the Internet, select Everyone.

b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.

c. To allow access from a single IP address on the Internet, select Only this computer. Enter the IP address that will be allowed access.

3. Specify the Port Number that will be used for accessing the management interface.

   web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click **Apply** to have your changes take effect.

**Note:** When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, you must enter *http://134.177.0.123:8080* in your browser.

# UPnP

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

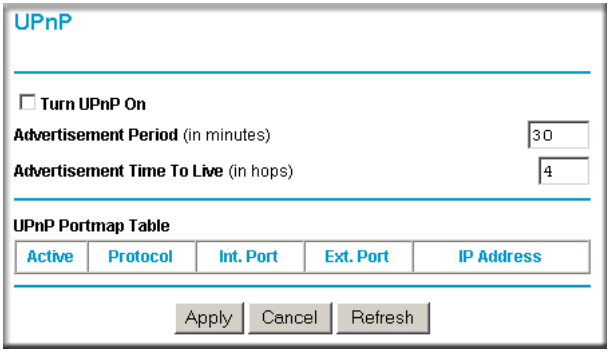



**Figure 6-8: UPnP page**

- Turn UPnP On: UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.
- Advertisement Period: The Advertisement Period is how often the router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
- Advertisement Time To Live: The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.
- UPnP Portmap Table: The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

# Syslog

Click Syslog on the Main Menu to view the Syslog page.

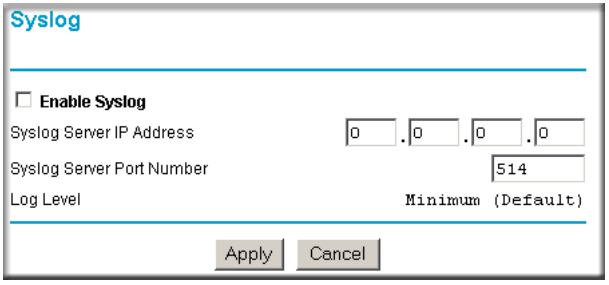



**Figure 6-9: Syslog page**

- Enable Syslog: Click the check box to Enable Syslog.
- Syslog Server Ip Address: When you enable syslog, fill server ip address.

- Syslog Server Port Number: Default value is 514.
- Log Level: The value may be:
  - .Minimum (Default)
  - .Middle
  - .Debug
  - .Full

## Firmware Upgrade

You install new versions of the router's software using the Router Upgrade page.

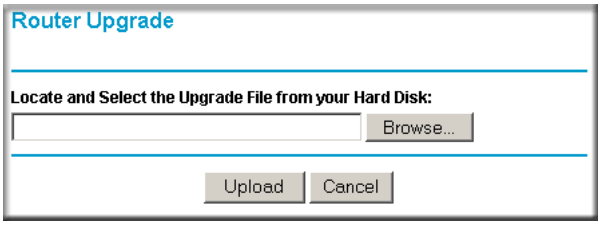



**Figure 6-10: Router Upgrade page**

Go to the NETGEAR Web site to get new versions of the router software. After downloading the file, you'll need to unzip (or unstuff) it before upgrading the router.

**IMPORTANT**! Once you click Upload do NOT interrupt the process of sending the software to the router and restarting the router. If you think the process may be interrupted in some way, click Cancel to keep the current router software.

To upgrade router software:

1. Go to www.NETGEAR.com and download the updated software.
2. If not done automatically, uncompress the file.

   You may want to read the Release Notes before continuing.
3. Click Browse.
4. Locate and select the file you just downloaded and uncompressed.
5. Click Upload to send the software to the router.

This loads the new software in the router and causes the router to restart.

**Note**: Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Ready light stops blinking, wait a few more seconds before doing anything.

6. Click Router Status and check the Firmware Version to verify that your router now has the new software installed.

   **IMPORTANT**! In some cases, such as a major upgrades, you may need to reconfigure your router after upgrading it. Refer to the Release Notes included with the software to find out if you need to reconfigure the router.

If you are unable to successfully upgrade using this method, refer to the Reference Manual on the Resource CD for other ways to upgrade the router.

# Chapter 7
# Troubleshooting

This chapter gives information about troubleshooting your TA612V Broadband Voice Adapter. After each problem description, instructions are provided to help you diagnose and solve the problem.

## Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power light is on.
2. After approximately 10 seconds, verify that:
   a. The power light is solid green.
   b. The LAN port lights are lit for any local ports that are connected.
   c. The Internet port light is lit.

   If a port's light is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's light is green. If the port is 10 Mbps, the light will be amber.

If any of these conditions does not occur, refer to the appropriate following section.

### Power Light Not On

If the Power and other lights are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

## Lights Never Turn Off

When the router is turned on, the lights turns on for about 10 seconds and then turn off. If all the lights stay on, there is a fault within the router.

If all lights are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.61.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 7-7.

If the error persists, you might have a hardware problem and should contact technical support.

## LAN or WAN Port Lights Not On

If either the LAN lights or Internet light do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:

  When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

# Troubleshooting the Web Configuration Interface

If you are unable to access the router's web Configuration interface from a computer on your local network, check the following:

- Check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.61.2 to 192.168.61.254.

  **Note:** If your computer's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address has been changed and you don't know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.61.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 7-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the web browser. The changes may have occurred, but the web browser may be caching the old configuration.

# Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should first determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com
2. Access the Main Menu of the router's configuration at http://192.168.61.1
3. Under the Maintenance heading, select Router Status
4. Check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new router by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your router.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem's lights indicate that it has reacquired sync with the ISP, reapply power to your router.
5. Then restart your computer.

If your router is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

OR

Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to "How to Manually Configure Your Internet Connection" on page 3-11.

If your router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. Alternatively, you may configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address.

# Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer or workstation.

## Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   **`ping 192.168.61.1`**

3. Click on OK.

You should see a message like this one:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port Lights Not On" on page 7-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows run menu, type:

**PING -n 10** *<IP address>*

where *<IP address>* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- — Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- — Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

— Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your computer, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer. Refer to "How to Manually Configure Your Internet Connection" on page 3-11.

## Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 192.168.61.1.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the power light blinks on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

   If the broadband voice adapter fails to restart or the power light continues to blink or turns solid amber, the unit may be defective. If the error persists, you might have a hardware problem and should contact technical support.

## Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The TA612V adapter uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked "Adjust for Daylight Savings Time".

# Appendix A
# Technical Specifications

This appendix provides technical specifications for the TA612V Broadband Voice Adapter.

| | |
|---|---|
| **Network Protocol and Standards Compatibility** | |
| Data and Routing Protocols: | TCP/IP, RIP-1, DHCP<br>PPP over Ethernet (PPPoE) |
| **Power Adapter** | |
| All regions (output): | 12V DC @ 1.5A output |
| **Environmental Specifications** | |
| Operating temperature: | 0° to 40° C (32º to 104º F) |
| Operating humidity: | 90% maximum relative humidity, noncondensing |
| **Electromagnetic Emissions** | |
| Meets requirements of: | FCC Part 15 Class B |
| **Interface Specifications** | The router incorporates Auto Uplink™ technology which eliminates the need for crossover cables. |
| LAN: | 10BASE-T or 100BASE-Tx, RJ-45, autosensing and capable of full-duplex or half-duplex operation. |
| WAN: | 10BASE-T or 100BASE-Tx, RJ-45, autosensing and capable of full-duplex or half-duplex operation. |

# Appendix B
# Network and Routing Basics

This chapter provides an overview of IP networks, routing, and networking.

## Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

## Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

### What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The TA612V Broadband Voice Adapter is a small office router that routes the IP protocol over a single-user broadband connection.

## Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The TA612V adapter supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

# IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

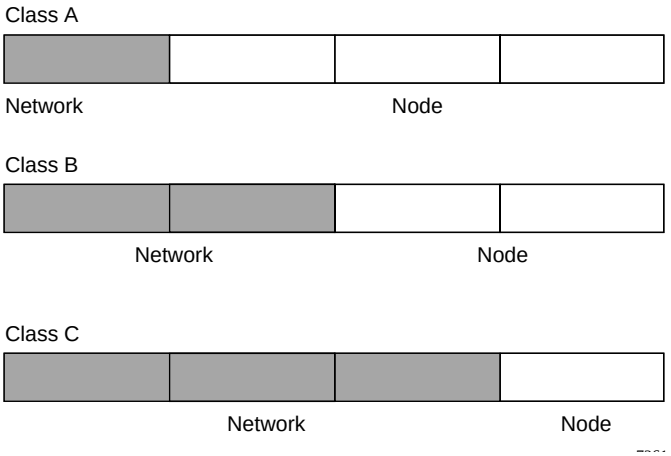



**Figure B-1: Three Main Address Classes**

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

## Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as "/n." In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

## Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

**Figure B-2: Example of Subnetting a Class B Address**

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

| | |
|---|---|
| | **Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet. |

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

**Table 7-1. Netmask Notation Translation Table for One Octet**

| Number of Bits | Dotted-Decimal Value |
|---|---|
| 1 | 128 |
| 2 | 192 |
| 3 | 224 |
| 4 | 240 |
| 5 | 248 |
| 6 | 252 |
| 7 | 254 |
| 8 | 255 |

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

**Table 7-2. Netmask Formats**

| Dotted-Decimal | Masklength |
|---|---|
| 255.0.0.0 | /8 |
| 255.255.0.0 | /16 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |
| 255.255.255.254 | /31 |
| 255.255.255.255 | /32 |

Configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

## Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Choose your private network number from this range. The DHCP server of the TA612V adapter is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its web site at www.ietf.org.

# Single IP Address Operation Using NAT

In the past, if multiple computers on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The TA612V adapter employs an address-sharing method called Network Address Translation (NAT). This method allows several networked computers to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

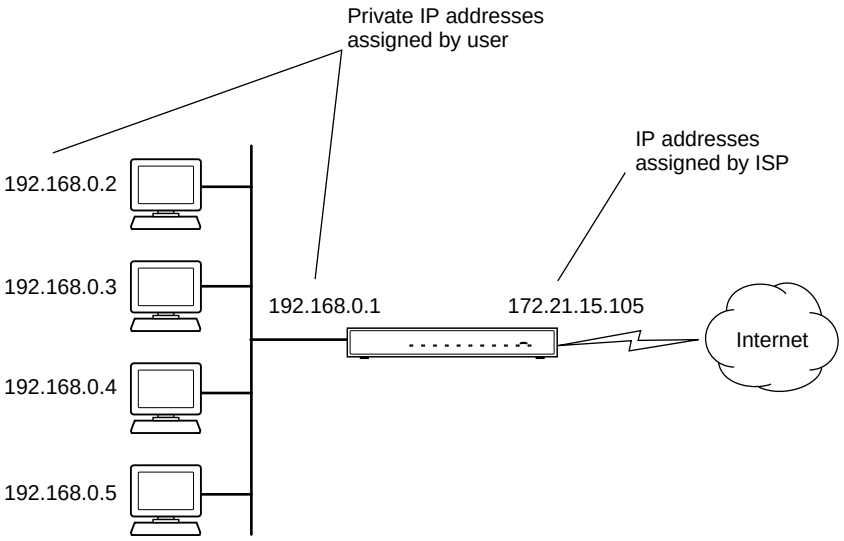



**Figure B-3: Single IP Address Operation Using NAT**

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one computer (for example, a web server) on your local network to be accessible to outside users.

## MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

## Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

## Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a computer accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The computer sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

# IP Configuration by DHCP

When an IP-based local area network is installed, each computer must be configured with an IP address. If the computers need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each computer on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The TA612V adapter has the capacity to act as a DHCP server.

The TA612V adapter also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

# Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the process, the network behind the router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

## What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker’s IP address for a period of time.

### Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

### Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

## Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table B-1.

**Table B-1. UTP Ethernet cable wiring, straight-through**

| Pin | Wire color | Signal |
|---|---|---|
| 1 | Orange/White | Transmit (Tx) + |
| 2 | Orange | Transmit (Tx) - |
| 3 | Green/White | Receive (Rx) + |
| 4 | Blue | |
| 5 | Blue/White | |
| 6 | Green | Receive (Rx) - |
| 7 | Brown/White | |
| 8 | Brown | |

## Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

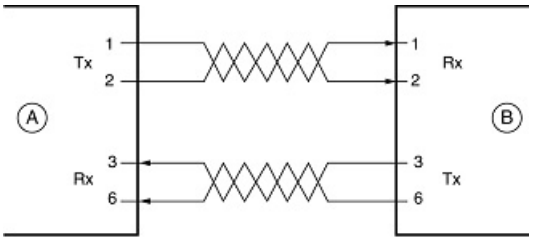
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

## Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

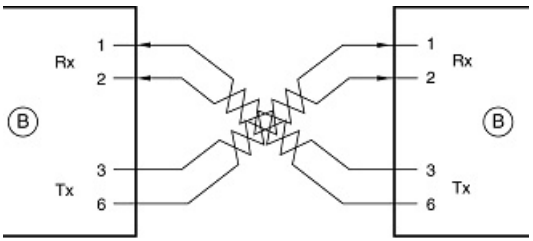
Figure B-4 illustrates straight-through twisted pair cable.




Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

**Figure B-4: Straight-Through Twisted-Pair Cable**

Figure B-5 illustrates crossover twisted pair cable.




Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

**Figure B-5: Crossover Twisted-Pair Cable**

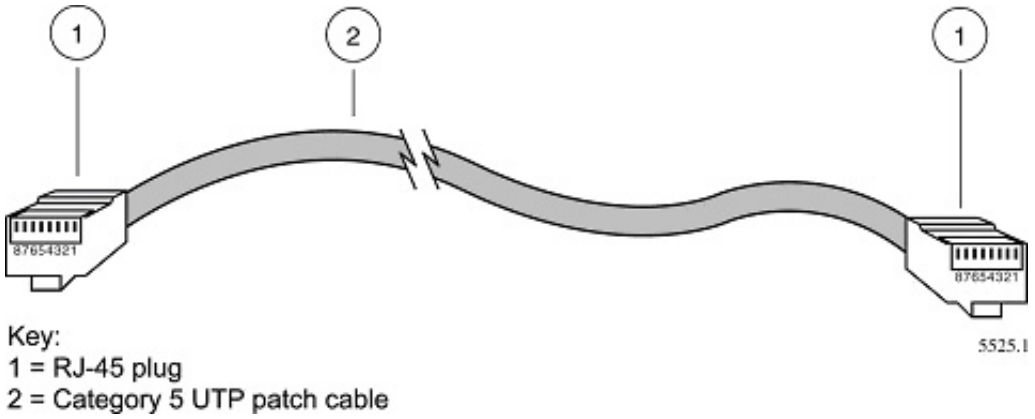



**Figure B-6: Category 5 UTP Cable with Male RJ-45 Plug at Each End**

**Note**: Flat "silver satin" telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

## Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the computer, which is wired as Media Dependant Interface (MDI). In this wiring, the computer transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a computer to a computer, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The TA612V adapter incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a computer) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

# Appendix C
# Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the TA612V Broadband Voice Adapter and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

**Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-21 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-22 for further information.

## What You Need To Use a Router with a Broadband Modem

You need to prepare these three things before you begin:

### Cabling and Computer Hardware

To use the TA612V adapter on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network using an Ethernet NIC at 100 Mbps, you must use a Category 5 (Cat 5) cable such as the one provided with your router. For an explanation of Ethernet cabling, see "Ethernet Cabling" on page B-11. The cable or DSL broadband modem must provide a standard 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx) Ethernet interface.

### Computer Network Configuration Requirements

The TA612V includes a built-in Web Configuration Manager. To access the configuration menus on the TA612V, your must use a Java-enabled Web browser program which supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer or Netscape Navigator 4.0 or above.

For the initial setup of your router, you will need to connect a computer to the router. This computer has to be set to automatically get its TCP/IP configuration from the router via DHCP.

**Note:** For help with DHCP configuration, please use the Windows TCP/IP Configuration Tutorials on the *NETGEAR CD*, or in this appendix.

## Internet Configuration Requirements

Depending on how your Internet service set up your account, you may need one or more of these configuration parameters to connect your router to the Internet:

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed IP Address which is also known as Static IP Address

## Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

- Your Internet service provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your Internet service to provide it or you can try one of the options below.
- If you have a computer already connected using the Internet, you can gather the configuration information from that computer.
  - — For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - — For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - — For Macintosh computers, record the settings in the TCP/IP or Network control panel.
- You may also refer to the *NETGEAR CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

## Record Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

**ISP Login Name:** The login name and password are case sensitive and must be entered exactly as given by your ISP. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, enter the following:

Login Name: _____

Password: _____

Service Name: _____

**Fixed or Static IP Address:** If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: _____ _____ _____ _____

Gateway IP Address: _____ _____ _____ _____

Subnet Mask: _____ _____ _____ _____

**ISP DNS Server Addresses:** If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: _____ _____ _____ _____

Secondary DNS Server IP Address: _____ _____ _____ _____

**Host and Domain Names:** Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

# Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your computer, then TCP/IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.

- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each computer and the firewall must be assigned a unique IP addresses. Each computer must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the computer obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Network and Routing Basics."

The TA612V adapter is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.61.2 through 192.168.61.253
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.61.1

These addresses are part of the IETF-designated private address range for use in private networks.

# Configuring Windows 95, 98, and Me for TCP/IP Networking

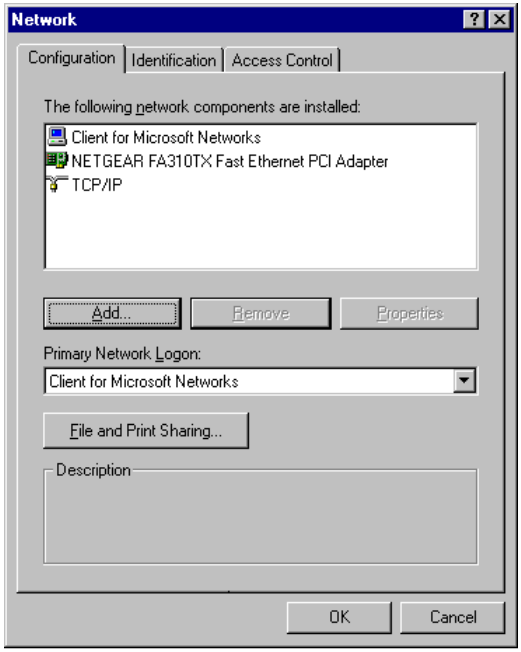
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

## Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:




You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

**Note:** It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

## Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

1

Locate your **Network Neighborhood** icon.

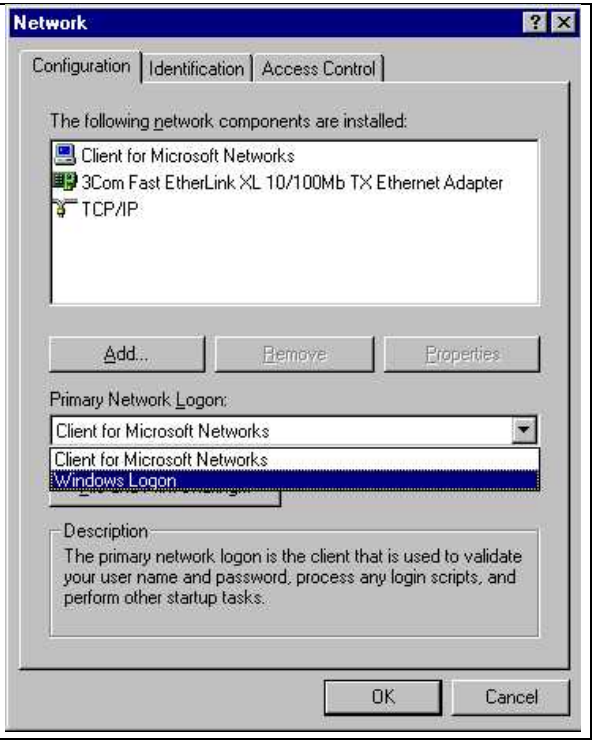
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

**2**

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.



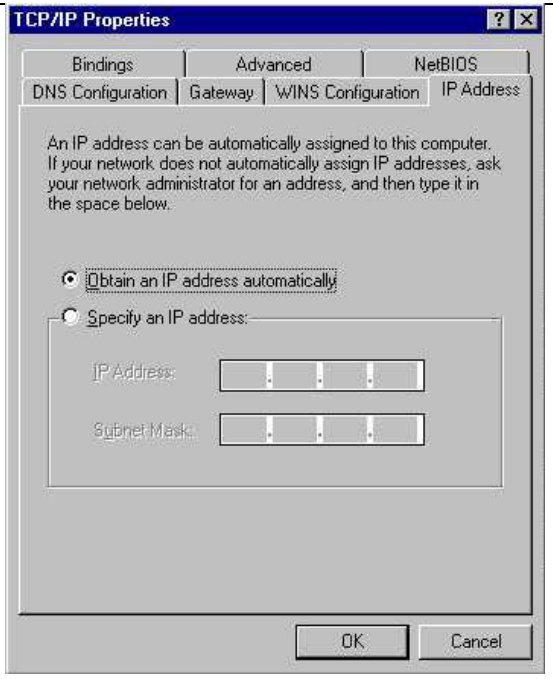
**3**

- By default, the **IP Address** tab is open on this window.
- Verify the following:

  **Obtain an IP address automatically** is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
- Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

## Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

## Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **winipcfg**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.61.2 and 192.168.61.253
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.61.1

# Configuring Windows NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

## Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Then, restart your PC.

## DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

## DHCP Configuration of TCP/IP in Windows XP

**1**

Locate your **Network Neighborhood** icon.

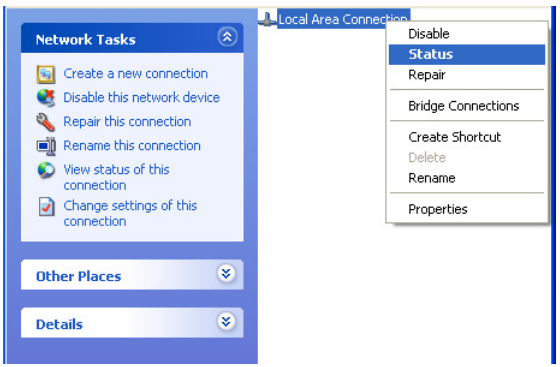
- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

**2**

- Now the Network Connection window displays.

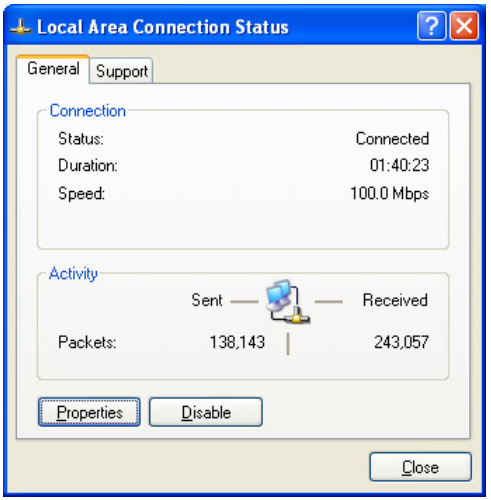
  The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the **Connection** you will use and choose **Status**.



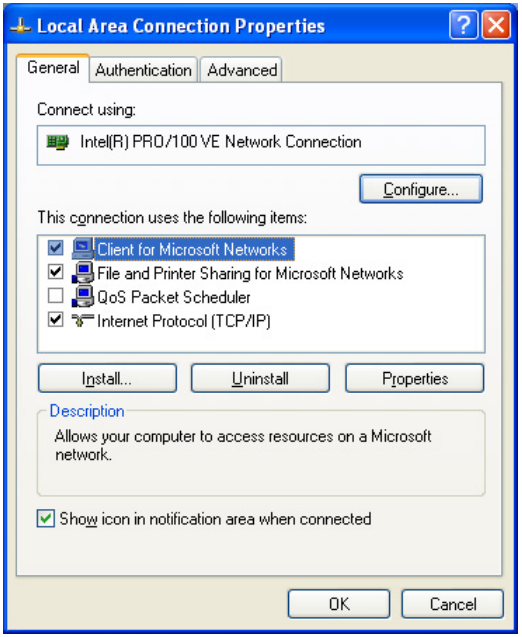
**3**

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.
- Administrator logon access rights are needed to use this window.
- Click the **Properties button** to view details about the connection.




**4**

- The TCP/IP details are presented on the Support tab page.
- Select **Internet Protocol,** and click **Properties** to view the configuration information**.**

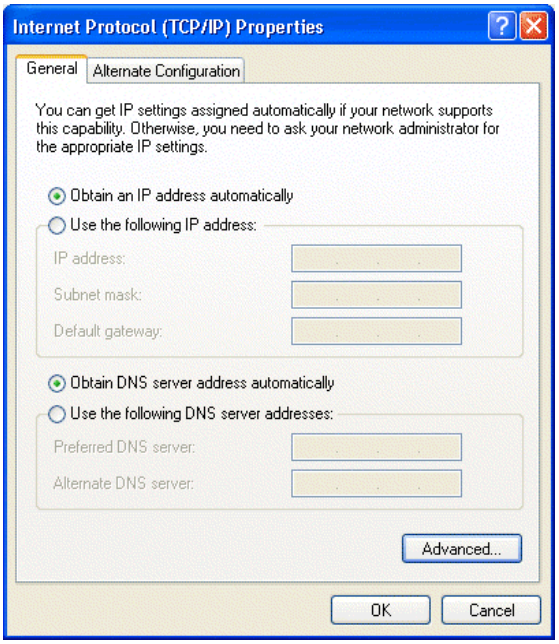


**5**

- Verify that the **Obtain an IP address automatically** radio button is selected.
- Verify that **Obtain DNS server address automatically** radio button is selected.
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

## DHCP Configuration of TCP/IP in Windows 2000

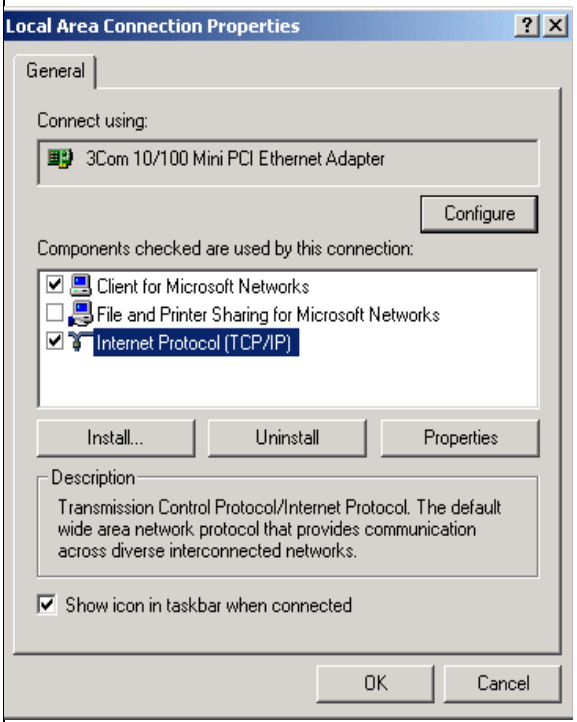
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

**1**

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on **Local Area Connection** and select **Properties**.

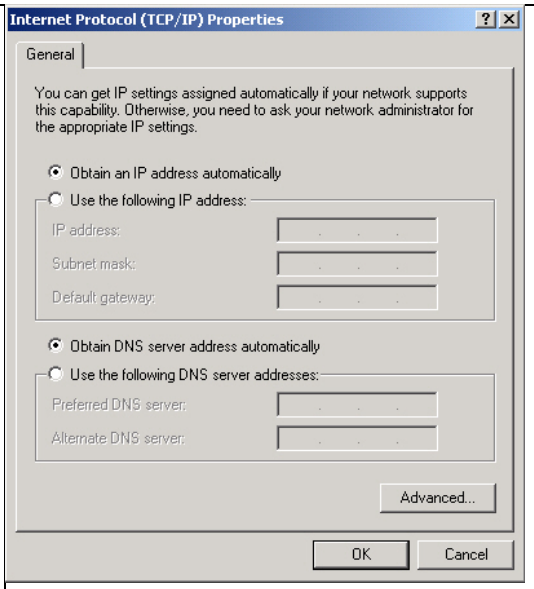
**2**

- The **Local Area Connection Properties** dialog box appears.
- Verify that you have the correct Ethernet card selected in the **Connect using:** box.
- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"
  - Client for Microsoft Networks and
  - Internet Protocol (TCP/IP)
- Click **OK**.



**3**

- With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box.
- Verify that
  - **Obtain an IP address automatically** is selected.
  - **Obtain DNS server address automatically** is selected.
- Click **OK** to return to Local Area Connection Properties.

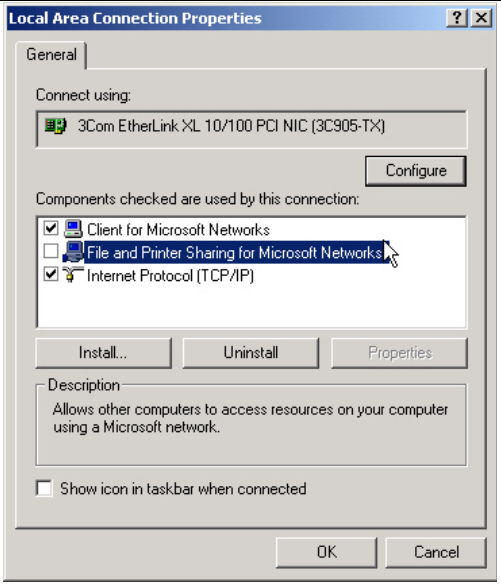

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

**4**

- Click **OK** again to complete the configuration process for Windows 2000.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



## DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

**1**

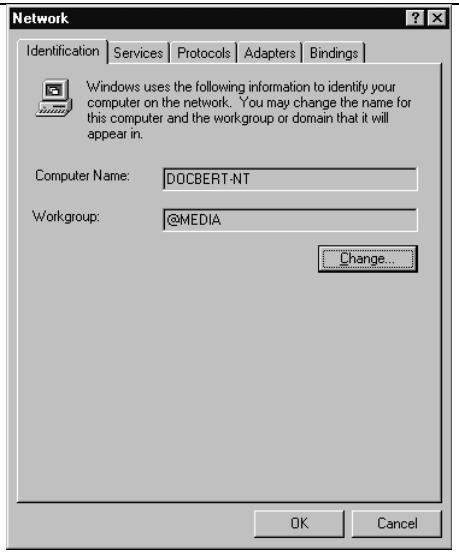
- Choose **Settings** from the Start Menu, and then select **Control Panel**. This will display Control Panel window.

**2**

- Double-click the **Network** icon in the Control Panel window.

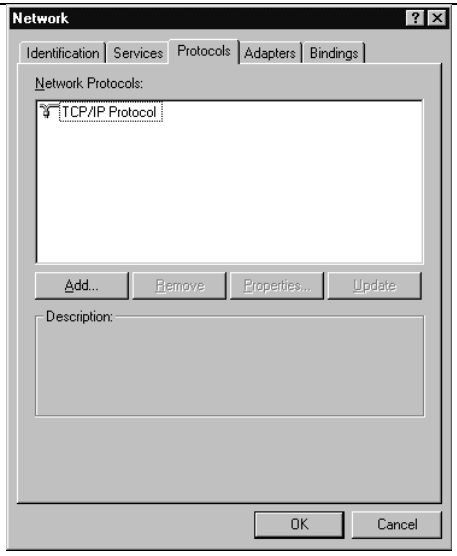
  The Network panel will display.

- Select the **Protocols** tab to continue.



**3**

- Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.

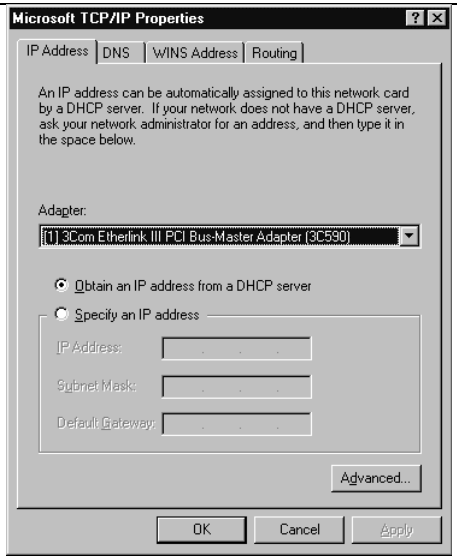


**4**

- The **TCP/IP Properties** dialog box now displays.
- Click the **IP Address** tab**.**
- Select the radio button marked **Obtain an IP address from a DHCP server.**
- Click **OK**. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] 3Com Etherlink III PCI Bus-Master Adapter (3C590)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

## Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type **`cmd`** and then click OK.

   A command window opens

3. Type **`ipconfig /all`**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.61.2 and 192.168.61.254
   - The subnet mask is 255.255.255.0

- The default gateway is 192.168.61.1

4. Type **`exit`**

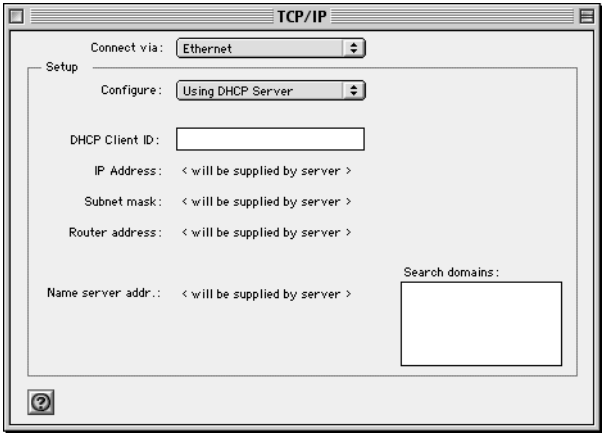
# Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

## MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens:




2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.

4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

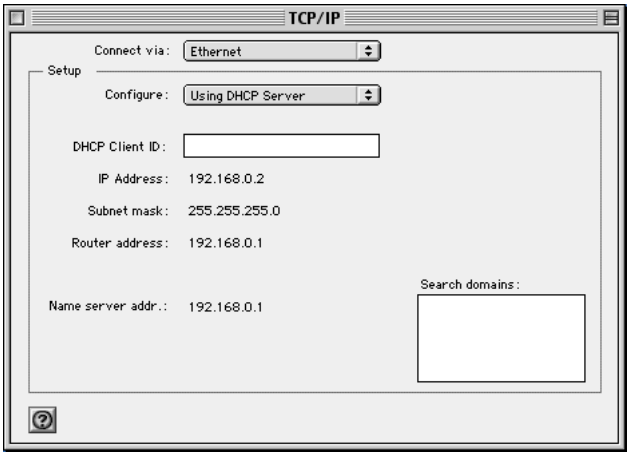
## MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

## Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.




The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.61.2 and 192.168.61.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.61.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

# Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall's Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

## Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router's configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

## What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

## Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the TA612V adapter. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".
5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

## Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the TA612V adapter. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

## Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your TA612V adapter, you are ready to access and configure the firewall.

# Glossary

Use the list below to find definitions for technical terms used in this manual.

## List of Glossary Terms

**10BASE-T**
IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

**100BASE-Tx**
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

**802.1x**
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.
The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

**802.11a**
IEEE specification for wireless networking at 54 Mbps operating in unlicensed radio bands over 5GHz.

**802.11b**
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.

**802.11g**
A soon to be ratified IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz. 802.11g is backwards compatible with 802.11b.

**ADSL**
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

**AES**

Advanced Encryption Standard, a symmetric 128-bit block data encryption technique.
It is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

**ARP**

Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address.
A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

**Auto Uplink**

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

**Cat 5**

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).
This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

**Denial of Service attack**

DoS. A hacker attack designed to prevent your computer or network from operating or communicating.

**DHCP**

An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

**DMZ**

A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.

The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

**DNS**

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

**Domain Name**

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

**DoS**

A hacker attack designed to prevent your computer or network from operating or communicating.

**DSL**

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

**DSLAM**

DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

**Dynamic Host Configuration Protocol**

DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

**EAP**

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.

EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and

transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

**ESP**
Encapsulating Security Payload.

**ESSID**
The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

**Gateway**
A local device, usually a router, that connects hosts on a local network to other networks.

**IETF**
Internet Engineering Task Force. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at *www.ietf.org*.
An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

**IP**
Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

**IP Address**
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
Ranges of addresses are assigned by Internic, an organization formed for this purpose.

**IPX**
Short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems.
Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services.

**ISP**
Internet service provider.

**Internet Protocol**
The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

**LAN**
A communications network serving users within a limited area, such as one floor of a building.

**LDAP**
A set of protocols for accessing information directories.

**Lightweight Directory Access Protocol**
LDAP. A set of protocols for accessing information directories.
LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called *X.500-lite.*

**local area network**
LAN. A communications network serving users within a limited area, such as one floor of a building.
A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

**MAC address**
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

**Mbps**
Megabits per second.

**MDI/MDIX**
In cable wiring, the concept of transmit and receive are from the perspective of the computer, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a computer transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See also AES.

**Maximum Receive Unit**
The size in bytes of the largest packet that can be sent or received.

**Maximum Transmit Unit**
The size in bytes of the largest packet that can be sent or received.

**Most Significant Bit or Most Significant Byte**
MSB. The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

**MRU**
The size in bytes of the largest packet that can be sent or received.

**MSB**
MSB. The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

**MTU**
The size in bytes of the largest packet that can be sent or received.

**NAT**
A technique by which several hosts share a single IP address for access to the Internet.

**NetBIOS**
The Network Basic Input Output System is an application programming interface (API) for sharing services and information on local-area networks (LANs).
Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, up to 16 characters in length.

**Network Address Translation**
NAT. A technique by which several hosts share a single IP address for access to the Internet.

**NIC**
Network Interface Card. An adapter in a computer which provides connectivity to a network.

**NID**
Network Interface Device. The point of demarcation, where the telephone line comes into the house.

**packet**
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

**Perfect Forward Secrecy**
Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

**PKIX**
PKIX. The most widely used standard for defining digital certificates.

**Point-to-Point Protocol**
PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

**PPP**
A protocol allowing a computer using TCP/IP to connect directly to the Internet.

**PPPoA**
PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

**PPPoE**
PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

**PPP over ATM**
PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

**PPP over Ethernet**
PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

**PPTP**
Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.

**PSTN**
Public Switched Telephone Network.

**RADIUS**
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.
Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

**RFC**
Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

**RIP**
A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

**router**
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

**Routing Information Protocol**
RIP. A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

**router**
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

**SSID**
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.
This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

**Subnet Mask**
A mask used to determine what subnet an IP address belongs to. Subnetting enables a network administrator to further divide an IP address into two or more subnets.
An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.
Subnetting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. This is easier to see if we show the IP address in binary format. The full address is: 10010110.11010111.00010001.00001001
The Class B network part is: 10010110.11010111
and the host address is 00010001.00001001
If this network is divided into 14 subnets, however, then the first 4 bits of the host address (0001) are reserved for identifying the subnet.

The subnet mask is the network address plus the bits reserved for identifying the subnetwork. (By convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address.) In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a mask because it can be used to identify the subnet to which an IP address belongs by performing a bitwise AND operation on the mask and the IP address. The result is the subnetwork address: Subnet Mask 255.255.240.000 11111111.11111111.11110000.00000000
IP Address 150.215.017.009 10010110.11010111.00010001.00001001
Subnet Address 150.215.016.000 10010110.11010111.00010000.00000000

The subnet address, therefore, is 150.215.016.000.

**TCP/IP**
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

**TLS**
Short for Transport Layer Security, TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.

The TLS protocol is made up of two layers. The TLS Record Protocol ensures that a connection is private by using symmetric data encryption and ensures that the connection is reliable. The second TLS layer is the TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before data is transmitted or received. Based on Netscape's SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

**Universal Plug and Play**

UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

**UTP**

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

**WAN**

A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

**WEB Proxy Server**

A web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall.
The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

**WEP**

Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

**wide area network**

WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

**Wi-Fi**

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

**Windows Internet Naming Service**

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

**WINS**

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

**Wireless Network Name (SSID)**

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

**WPA**

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.